

INFINITE RANK OF ELLIPTIC CURVES OVER \mathbb{Q}^{ab}

BO-HAE IM AND MICHAEL LARSEN

ABSTRACT. If E is an elliptic curve defined over a quadratic field K , and the j -invariant of E is not 0 or 1728, then $E(\mathbb{Q}^{\text{ab}})$ has infinite rank. If E is an elliptic curve in Legendre form, $y^2 = x(x-1)(x-\lambda)$, where $\mathbb{Q}(\lambda)$ is a cubic field, then $E(K\mathbb{Q}^{\text{ab}})$ has infinite rank. If $\lambda \in K$ has a minimal polynomial $P(x)$ of degree 4 and $v^2 = P(u)$ is an elliptic curve of positive rank over \mathbb{Q} , we prove that $y^2 = x(x-1)(x-\lambda)$ has infinite rank over $K\mathbb{Q}^{\text{ab}}$.

1. INTRODUCTION

In [2], G. Frey and M. Jarden proved that every elliptic curve E/\mathbb{Q} has infinite rank over \mathbb{Q}^{ab} and asked whether the same is true for all abelian varieties. For a general number field K (not necessarily contained in \mathbb{Q}^{ab}), the question would be whether every abelian variety A over K is of infinite rank over $K\mathbb{Q}^{\text{ab}}$. An affirmative answer to this question would follow from an affirmative answer to the original question, since every \mathbb{Q}^{ab} -point of the Weil restriction of scalars $\text{Res}_{K/\mathbb{Q}}A$ gives a $K\mathbb{Q}^{\text{ab}}$ -point of A . We specialize the question to dimension 1.

Question 1. *If E is an elliptic curve over a number field K , must E have infinite rank over $K\mathbb{Q}^{\text{ab}}$?*

Specializing further to the case that K is abelian over \mathbb{Q} , the question can be reformulated as:

Question 2. *Does every elliptic curve over \mathbb{Q}^{ab} have infinite rank over \mathbb{Q}^{ab} ?*

In a recent paper [6], E. Kobayashi considered Question 2 when $[K : \mathbb{Q}]$ is odd. In this setting, she gave an affirmative answer, conditional on the Birch-Swinnerton-Dyer conjecture.

We give an affirmative answer to Question 1 when E is defined over a field K of degree ≤ 4 over \mathbb{Q} and satisfies some auxiliary condition.

Date: February 8, 2012.

2000 Mathematics Subject Classification. 11G05.

Bo-Hae Im was supported by the National Research Foundation of Korea Grant funded by the Korean Government(MEST) (NRF-2011-0015557). Michael Larsen was partially supported by NSF grants DMS-0800705 and DMS-1101424.

In all of our results, we can replace \mathbb{Q}^{ab} by $\mathbb{Q}(2)$, the compositum of all quadratic extensions of \mathbb{Q} . Our strategy for finding points over $\mathbb{Q}(2)$ entails looking for \mathbb{Q} -points on the Kummer variety $\text{Res}_{K/\mathbb{Q}}E/(\pm 1)$ by looking for curves of genus ≤ 1 on that variety. When K is a quadratic field, $\text{Res}_{K/\mathbb{Q}}E$ is an abelian surface isomorphic, over \mathbb{C} , to a product of two elliptic curves. Our construction of a curve on the Kummer surface $\text{Res}_{K/\mathbb{Q}}E/(\pm 1)$ is modelled on the construction of a rational curve on $(E_1 \times E_2)/(\pm 1)$ due to J-F. Mestre [7] and to M. Kuwata and L. Wang [5]. For $[K : \mathbb{Q}] = 3$, our proof depends on an analogous construction of a rational curve on $(E_1 \times E_2 \times E_3)/(\pm 1)$ which is presented in [4]. We do not know of any rational curve on $(E_1 \times E_2 \times E_3 \times E_4)/(\pm 1)$ for generic choices of the E_i , but [4] constructs a curve of genus 1 in this variety.

2. A GEOMETRIC CONSTRUCTION

We now recall a geometric construction of a curve in

$$(1) \quad (E_1 \times \cdots \times E_n)/(\pm 1),$$

where (± 1) acts diagonally on the product.

Lemma 3. *Let \bar{K} be a separably closed field with $\text{char}(\bar{K}) \neq 2$ and for an integer $n \geq 2$, let E_1, \dots, E_n be pairwise non-isomorphic elliptic curves over \bar{K} . Then $E_1 \times \cdots \times E_n)/(\pm 1)$ contains a curve X whose normalizer has genus*

$$g_n := 2^{n-3}(n-4) + 1.$$

In particular, $g_2 = g_3 = 0$ and $g_4 = 1$.

Proof. Let E_i be written in Legendre form : for $i = 1, 2, \dots, n$,

$$E_i : y_i^2 = x_i(x_i - 1)(x_i - \lambda_i), \quad \lambda_i \in \bar{K}.$$

Since the E_i are non-isomorphic over \bar{K} , the λ_i are distinct.

Considering $E_1 \times \cdots \times E_n$ as a $(\mathbb{Z}/2\mathbb{Z})^n$ -cover of

$$E_1/(\pm 1) \times \cdots \times E_n/(\pm 1) \cong (\mathbf{P}^1)^n,$$

we examine the inverse image in (1) of \mathbf{P}^1 embedded diagonally in $(\mathbf{P}^1)^n$.

An affine open set of the resulting curve has coordinate ring

$$\begin{cases} z_{12}^2 &= x^2(x-1)^2(x-\lambda_1)(x-\lambda_2) \\ &\vdots \\ z_{1n}^2 &= x^2(x-1)^2(x-\lambda_1)(x-\lambda_n), \end{cases}$$

with $z_{12} = y_1 y_2, \dots, z_{1n} = y_1 y_n$ fixed under the action of (± 1) . A projective non-singular model is given in homogeneous coordinates by

$$C_n : \begin{cases} u_1^2 &= (v - \lambda_1 t)(v - \lambda_2 t), \\ &\vdots \\ u_{n-1}^2 &= (v - \lambda_1 t)(v - \lambda_n t). \end{cases}$$

Then by the Riemann-Hurwitz formula, the genus g_n of C_n is given by

$$2g_n - 2 = 2^{n-1}(-2) + n2^{n-2}.$$

If $n = 2$ or $n = 3$, then $g_n = 0$ and if $n = 4$, then $g_n = 1$. This completes the proof. \square

It is difficult to tell when this construction produces a curve with infinitely many rational points over \mathbb{Q} . We do not use Lemma 3 directly in what follows, but it motivates the apparently *ad hoc*, explicit constructions of the remainder of the paper. Each of the following sections deals with them and the quadratic case in Section 3 shows a concrete construction which motivates other cases.

3. THE QUADRATIC CASE

We begin with a lemma.

Lemma 4. *Let k be a non-negative integer and $Q(u, v) \in \mathbb{Q}[u, v]$ a homogeneous polynomial of degree $2(2k+1)$ satisfying the functional equation*

$$Q(mu, v) = m^{2k+1}Q(v, u)$$

for a fixed squarefree integer $m \neq 1$. Then $Q(u, v)$ cannot be a perfect square in $\mathbb{C}[u, v]$.

Proof. Let i be the largest integer such that v^i divides $Q(u, v)$. If i is odd, $Q(u, v)$ cannot be a perfect square in $\mathbb{C}[u, v]$. We therefore assume that $i = 2j$. Without loss of generality, we may assume that the $u^{4k+2-2j}v^{2j}$ coefficient is 1. If $q(u, v)$ is a square root of $Q(u, v)$ over \mathbb{C} , then the $u^{2k+1-j}v^j$ -coefficient of $q(u, v)$ is ± 1 . Every automorphism σ of the complex numbers sends $q(u, v)$ to $\pm q(u, v)$. However, σ fixes the $u^{2k+1-j}v^j$ coefficient of $q(u, v)$, so σ fixes $q(u, v)$, which means $q(u, v) \in \mathbb{Q}[u, v]$. From the given functional relation, $q(u, v)$ satisfies

$$q(mu, v) = \pm \sqrt{m}(m^k q(v, u)),$$

which gives a contradiction since $\sqrt{m} \notin \mathbb{Q}$. \square

Theorem 5. *Let $E: y^2 = P(x) := x^3 + \alpha x + \beta$ be an elliptic curve defined over a quadratic extension K of \mathbb{Q} . If the j -invariant of E is not 0 or 1728, then $E(\mathbb{Q}^{ab})$ has infinite rank.*

Proof. Let $K = \mathbb{Q}(\sqrt{m})$, where $m \in \mathbb{Z}$ is a square-free integer, and $E: y^2 = P(x) := x^3 + \alpha x + \beta$ an elliptic curve defined over K . By the hypothesis on the j -invariant, $\alpha \neq 0$ and $\beta \neq 0$. Replacing α and β by $\lambda^4\alpha$ and $\lambda^6\beta$ for suitable $\lambda \in K$, we may assume without loss of generality that $\alpha, \beta \notin \mathbb{Q}$.

Let $\alpha = a + c\sqrt{m}$ and $\beta = b + d\sqrt{m}$ for $a, b, c, d \in \mathbb{Q}, c, d \neq 0$. Then for $x_1 := -\frac{d}{c} \in \mathbb{Q}$, we have $P(x_1) \in \mathbb{Q}$, and

$$(x_1, \sqrt{P(x_1)}) \in E(K(\sqrt{P(x_1)})) \subseteq E(\mathbb{Q}^{ab}).$$

Now by substituting α by $\gamma^4\alpha$ and β by $\gamma^6\beta$ for $\gamma \in K$ such that $\gamma^4\alpha, \gamma^6\beta \notin \mathbb{Q}$, we get an isomorphism over K between E and the elliptic curve

$$E_\gamma: y^2 = P_\gamma(x) := x^3 + \gamma^4\alpha x + \gamma^6\beta.$$

For each such $\gamma = u + v\sqrt{m}$ for $u, v \in \mathbb{Q}$, we get a point

$$(2) \quad \left(\gamma^{-2}x_\gamma, \gamma^{-3}\sqrt{P_\gamma(x_\gamma)} \right) \in E\left(K\left(\sqrt{P(x_\gamma)}\right)\right) \subseteq E(\mathbb{Q}^{ab}),$$

where $x_\gamma \in \mathbb{Q}$ and $P_\gamma(x_\gamma) \in \mathbb{Q}$.

Now we show that there are infinitely many quadratic fields L such that $\mathbb{Q}(\sqrt{P_\gamma(x_\gamma)}) = L$ for some $\gamma \in K$.

For $x \in \mathbb{Q}$, we expand $P_\gamma(x)$ as $R + I\sqrt{m}$ where $R, I \in \mathbb{Q}[u, v, x]$ and we get

$$I = xT_1(u, v) + S_1(u, v) \text{ and } R = x^3 + xT_2(u, v) + S_2(u, v),$$

where T_i and S_i are homogeneous polynomials in u and v over \mathbb{Q} of degree 4 and 6 respectively satisfying relations:

$$(3) \quad T_i(mu, v) = m^2T_i(v, u), \quad S_i(mu, v) = m^3S_i(v, u).$$

We solve the equation $I = xT_1(u, v) + S_1(u, v) = 0$ for x and get

$$x_\gamma = -\frac{S_1(u, v)}{T_1(u, v)}.$$

We then substitute this value of x into the rational part R of $P_\gamma(x)$, and after clearing the denominator by multiplying by the square $(T_1(u, v))^4$, we obtain the polynomial

$$-T_1(u, v)(S_1(u, v)^3 + S_1(u, v) T_1(u, v)^2 T_2(u, v) - S_2(u, v) T_1(u, v)^3),$$

which we denote Q . Thus, Q is homogeneous of degree 22 over \mathbb{Q} and from the relation (3), it satisfies

$$(4) \quad Q(mu, v) = m^{11}Q(v, u).$$

Note that by direct computation, the coefficients of the u^{22} -term and $u^{21}v$ -term in $Q(u, v)$ are respectively,

$$A_0 = c(-d^3 - adc^2 + bc^3), \quad A_1 = 2(-6a^2dc^2 - 2ad^3 + 5abc^3 + mc^4d - 9cd^2b).$$

If $Q(u, v) = 0$, then $A_0 = A_1 = 0$. Since $c \neq 0$ and $d \neq 0$, we solve $A_0 = 0$ for a and substitute

$$a = \frac{bc^3 - d^3}{c^2d}$$

into $A_1 = 0$. Then we get

$$-b^2c^6 - 4c^3d^3b - 4d^6 + mc^6d^2 = 0,$$

whose discriminant in b is $mc^{12}d^2$ which is not a square in \mathbb{Q} . Hence $A_1 \neq 0$. This shows that $Q(u, v)$ cannot be identically zero. By Lemma 4, $Q(u, v)$ cannot be a perfect square in $\mathbb{C}[u, v]$.

Hence $y^2 - Q(u, v)$ is irreducible over \mathbb{C} .

Let $f(t) \in \mathbb{Q}[t]$ be the polynomial of degree 22 in the variable $t = u/v$ obtained by replacing $Q(u, v)$ by $Q(u, v)v^{-22}$. For a finite extension L of K , we let

$$H(f, L) := \{t' \in \mathbb{Q} : f(t') - y^2 \text{ is irreducible over } L\}$$

the intersection of \mathbb{Q} with the Hilbert set of f over L . By the Hilbert irreducibility theorem ([3, Chapter 12]), such an intersection is non-empty.

Hence there exists $\gamma_0 = u_0 + v_0\sqrt{m} \in K$ such that

$$L_0 := \mathbb{Q}\left(\sqrt{P_{\gamma_0}(x_{\gamma_0})}\right) = \mathbb{Q}\left(\sqrt{Q(u_{\gamma_0}, v_{\gamma_0})}\right)$$

is a quadratic field not contained in L . Inductively, we get an infinite sequence of $\gamma_k = u_k + v_k\sqrt{m}$ such that the fields

$$L_k = \mathbb{Q}\left(\sqrt{P_{\gamma_k}(x_{\gamma_k})}\right) = \mathbb{Q}\left(\sqrt{Q(u_{\gamma_k}, v_{\gamma_k})}\right)$$

are all linearly disjoint.

Let V be the set

$$V := \left\{ \left(\gamma_k^{-2}x_{\gamma_k}, \gamma_k^{-3}\sqrt{P_{\gamma_k}(x_{\gamma_k})} \right) \in E\left(K\left(\sqrt{P(x_{\gamma_k})}\right)\right) \right\}_{k=0}^{\infty}.$$

By [8, Lemma], the set $\bigcup_{[L:K] \leq d} E(L)_{\text{tor}}$ is a finite set, where the union runs all over finite extensions L of K whose degree over K is less

than or equal to d . Therefore, V contains only finitely many torsion points. Then by linear disjointness of KL_i over K , non-torsion points $(\gamma_k^{-2}x_{\gamma_k}, \gamma_k^{-3}\sqrt{P_{\gamma_k}}(x_{\gamma_k})) \in V$ are linearly independent in $E(K\mathbb{Q}^{ab})$. Therefore the rank of $E(K\mathbb{Q}(2))$ is infinite, therefore, the rank of $E(K\mathbb{Q}^{ab}) \subseteq E(\mathbb{Q}^{ab})$ is infinite. \square

4. THE CUBIC CASE

Theorem 6. *Let λ denote an element of a cubic extension K of \mathbb{Q} . Then $E: y^2 = x(x-1)(x-\lambda)$ has infinite rank over $K\mathbb{Q}^{ab}$.*

Proof. If $\lambda \in \mathbb{Q}$, then we are done, so we assume that $\mathbb{Q}(\lambda) = K$.

Let

$$L(t) := t^3 - at^2 + bt - c$$

denote the minimal polynomial of λ . Expanding, we have

$$\left(\frac{b-t^2}{2} + (t-a)\lambda + \lambda^2\right)^2 = M(t) - L(t)\lambda,$$

where

$$M(t) := \frac{t^4 - 2bt^2 + 8ct + b^2 - 4ac}{4}.$$

Let

$$N(t) := L(t)M(t)(M(t) - L(t)).$$

Defining

$$\begin{aligned} x &:= \frac{M(t)}{L(t)}, \\ y &:= \frac{\left(\frac{b-t^2}{2} + (t-a)\lambda + \lambda^2\right)}{L(t)^2} \sqrt{N(t)}, \end{aligned}$$

we verify by computation that $(x, y) \in K(t, \sqrt{N(t)})^2$ lies on E , i.e., belongs to $E(K(t, \sqrt{N(t)}))$. Note that $\deg N = 11$, so $w^2 - N(t)$ is irreducible in $\mathbb{C}[w, t]$. Specializing t in \mathbb{Q} , and applying Hilbert irreducibility, as before, we obtain points of $E(KL_i)$ for an infinite sequence of quadratic fields L_i/\mathbb{Q} . It follows that E has infinite rank over $K\mathbb{Q}(2)$ and therefore over $K\mathbb{Q}^{ab}$. \square

5. THE QUARTIC CASE

Theorem 7. *Let λ denote an element generating a quartic extension K of \mathbb{Q} . Let $P(x)$ be the (monic) minimal polynomial of λ over \mathbb{Q} . If the genus 1 curve*

$$(5) \quad v^2 = P(u) := u^4 + pu^3 + qu^2 + ru + s$$

is an elliptic curve of positive rank over \mathbb{Q} , then $E: y^2 = x(x-1)(x-\lambda)$ has infinite rank over $K\mathbb{Q}^{\text{ab}}$.

Proof. If (u, v) satisfies (5), then setting

$$\begin{aligned} A(u, v) &= (2u^4 + pu^3 - ru - 2s)v \\ &\quad + \frac{8u^6 + 8pu^5 + (p^2 + 4q)u^4 - (8s + 2pr)u^2 - 8psu + r^2 - 4qs}{4}, \end{aligned}$$

$$\begin{aligned} B(u, v) &= (4u^3 + 3pu^2 + 2qu + r)v \\ &\quad + 4u^5 + 5pu^4 + (p^2 + 4q)u^3 + (4r + pq)u^2 + (4s + rp)u + ps, \end{aligned}$$

and

$$C(u, v) := \frac{-2uv - 2u^3 - pu^2 + r}{2} + (v + u^2 + pu + q)\lambda + (u + p)\lambda^2 + \lambda^3,$$

we have

$$C(u, v)^2 = A(u, v) - B(u, v)\lambda$$

by explicit computation. Thus, if $(u, v) \in \mathbb{Q}^2$, we have

$$\begin{aligned} (6) \quad P_{(u,v)} &:= \left(\frac{A(u, v)}{B(u, v)}, C(u, v) \sqrt{\frac{A(u, v)(A(u, v) - B(u, v))}{B(u, v)^3}} \right) \\ &\in E \left(K\mathbb{Q} \left(\sqrt{D(u, v)} \right) \right), \end{aligned}$$

where

$$D(u, v) := A(u, v)B(u, v)(A(u, v) - B(u, v)) \in \mathbb{Q}[u, v].$$

We embed the function field F of (5) in the field of Laurent series $F_\infty := \mathbb{C}((t))$ by mapping u to $1/t$ and v to the square root of $P(u)$ in $\mathbb{C}((t))$ with principal term $1/t^2$. We choose the correct square root of $P(u)$ so that this defines a discrete valuation on F with respect to which $A(u, v)$, $B(u, v)$ and $A(u, v) - B(u, v)$ have value 6, 5, and 6 respectively. It follows that $F_\infty(\sqrt{D(u, v)}) = \mathbb{C}((t^{1/2}))$. This implies that $\sqrt{D(u, v)}$ does not lie in F . Therefore, $\sqrt{D(u, v)} \notin F$. Let X denote the projective non-singular curve over \mathbb{C} with function field $F[z]/(z^2 - D(u, v))$. Then there exists a morphism from X to the projective non-singular curve with function field F , which is ramified

at F_∞ . It follows that the genus of X is at least 2. By Faltings' theorem [1], $X(\mathbb{Q}(\sqrt{D}))$ is finite for all $D \in \mathbb{Q}$. If there are infinitely many \mathbb{Q} -points $\{Q_k := (u_k, v_k)\}_{k=1}^\infty$ on (5), their inverse images generate infinitely many different quadratic extensions of \mathbb{Q} , and so the points $\{P_{(u_k, v_k)}\}_{k=1}^\infty$ of E in (6) are defined over different quadratic extensions $K\mathbb{Q}(\sqrt{D(u_k, v_k)})$ of \mathbb{Q} . By [8, Lemma] again, it follows that $E(K\mathbb{Q}(2))$ has infinite rank. \square

REFERENCES

- [1] Faltings, G.: Endlichkeitssätze für abelsche Varietäten über Zahlkörpern, *Invent. Math.* **73** (1983), 349–366.
- [2] G. Frey and M. Jarden, Approximation theory and the rank of abelian varieties over large algebraic fields, *Proc. London Math. Soc.* (3) **28**, 112–128 (1974).
- [3] M. D. Fried and M. Jarden, *Field arithmetic. Third edition. Revised by Jarden*. Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics, **11** (Springer-Verlag, Berlin), 2008.
- [4] Bo-Hae Im, Positive Rank Quadratic Twists of Four Elliptic Curves, preprint, 2011.
- [5] M. Kuwata and L. Wang, Topology of rational points on isotrivial elliptic surfaces, *Int. Math. Res. Notices.* **1993**, No.4, 113–123.
- [6] E. Kobayashi, A remark on the Mordell-Weil rank of elliptic curves over the maximal abelian extension of the rational number field, *Tokyo J. Math.* **V.29**, No. 2, 295–300 (2006).
- [7] J.-F. Mestre, Rang de courbes elliptiques d'invariant donné. *C. R. Acad. Sci. Paris Sér. I Math.* **314** (1992), no. 12, 919–922.
- [8] J. H. Silverman, Integer points on curves of genus 1, *J. London Math. Soc.* (2) **28**, (1983), 1–7.

DEPARTMENT OF MATHEMATICS, CHUNG-ANG UNIVERSITY, 221, HEUKSEOK-DONG, DONGJAK-GU, SEOUL, 156-756, SOUTH KOREA

E-mail address: imbh@cau.ac.kr

DEPARTMENT OF MATHEMATICS, INDIANA UNIVERSITY, BLOOMINGTON, INDIANA 47405, USA

E-mail address: mjlarsen@indiana.edu